AMENDMENTS TO THE SPECIFICATION:

Please delete the paragraph beginning at page 1, line 19 and replace with the following replacement paragraph:

As is known in the art, there is a trend to provide network processors that perform cryptographic processing of packet data. To facilitate cryptographic processing, network processors include cryptographic acceleration units (also referred to as "crypto units"). The crypto units accelerate the cryptographic processing of packet data to support cryptographic processing at line rate. One example of a network processor including such a crypto unit is the INTEL® ~~Intel~~ IXP2850 network processor manufactured by Intel Corporation of Santa Clara, CA.

Please delete the paragraph beginning at page 2, line 3 and replace with the following replacement paragraph:

The crypto units in the INTEL® ~~Intel~~ IXP2850 network processor, for example, implement the well-known 3DES/DES (Data Encryption Standard) and AES (Advanced Encryption Standard) cipher algorithms, as well as the SHA1 (Secure Hash Algorithm) authentication algorithm. Each of the crypto units contains a pair of 3DES/DES, and SHA1 cores and a single AES core. By implementing a pair of cores, the crypto units meet the data rate requirements by allowing both cores to process data in parallel, thereby doubling the data rate of a single core.

Please delete the paragraph beginning at page 4, line 4 and replace with the following replacement paragraph:

Data is moved to the crypto units 102 from one of the microengines (MEs) 104 or from the MSF (Media Switch Fabric) 105, which contains a receive buffer unit 106a and a transmit buffer unit 106b. As is well known to one of ordinary skill in the art, the MEs 104 are programmable packet processing engines that perform security protocol processing, as well as other functions. The crypto units 102 are controlled by software running on the MEs 104. The MSF unit 105 manages the interfaces 108, such as an SPI4 interface, ~~though~~ through which packet data enters and exits the network processor 100.

Please delete the paragraph beginning at page 5, line 5 and replace with the following replacement paragraph:

In an exemplary embodiment shown in FIG. 2, the crypto unit 102a has an authentication buffer 140 and a core containing four cipher cores: two 3DES cores 150, 152, an AES core 154, and an RC4 core 156, and five authentication cores: two MD5 cores 158, 160, two SHA1 cores 162, 164, and an AES-XCBC-MAC core 166. In order to support the ciphering of relatively small packets, the crypto units 102 each have six processing contexts 168a-168f, which are each used to process one data packet at a time. Each processing context 168 contains storage for the cipher keys and algorithm context associated with the processing of one packet. The multiple processing contexts 168 allow

the latency of loading cryptographic key material and packet data to be hidden by pipelining the loading of data and key material into some of the contexts with the processing of data in other contexts. This allows the crypto units ~~unit~~ 102 to achieve close to full utilization of the cipher and authentication cores.

Please delete the paragraph beginning at page 5, line 16 and replace with the following replacement paragraph:

In order to maximize ciphering and authentication processing data rates, the crypto unit ~~102~~ 102a performs both operations in one pass. Data is moved to the crypto unit ~~102~~ 102a with instructions as to which algorithms should be used and whether authentication should be performed before or after ciphering. If authentication is performed after ciphering (on the ciphered data), the crypto unit ~~102~~ 102a buffers the data in the authentication buffer 140 after it is ciphered and awaits processing by the given authentication core. If authentication is performed before ciphering or only authentication is performed, packet data enters the authentication buffer directly and awaits processing by the given authentication core.

Please delete the paragraph beginning at page 9, line 24 and replace with the following replacement paragraph:

While the embodiments described herein are primarily shown and described in conjunction with an INTEL® ~~Intel~~ IXP2850 network processor architecture, it is

understood that the disclosed embodiments are applicable to network processors in general. For example, it will be appreciated that any number of crypto units can be used without departing from the present embodiments. In addition, the number of cipher cores, authentication, and processing contexts, as well as the supported algorithm types and protocols and block and buffer element sizes can be readily varied without departing from the scope of the present embodiments.